
$$(r, s, t) \leftarrow \text{sign}(x, m)$$

(1) Choose $a, b \in_R \mathbb{Z}\mathbb{Z}_q$ such that $a + bm \neq -1 \pmod{q}$

(2) $r \leftarrow m^a g^a \pmod{p}$

if $r, r - mx$ or $(a + bm)r + mx = 0 \pmod{q}$, then repeat from step (1).

(3) $(s, t) \leftarrow (ar \frac{mx - r}{(a + bm)r + mx}, m \frac{r - mx}{(a + bm)r + mx})$

Fig. 1. Producing a signature

$$(m', (r', s', t')) \leftarrow \text{trans}(y, m, (r, s, t), \omega)$$

Bob

Verifier

(1) Choose $\alpha \in_R \mathbb{Z}\mathbb{Z}_q$

Choose $d \in_R \mathbb{Z}\mathbb{Z}_q^*$

(2) $m' \leftarrow m^\omega \pmod{p}$

(3) $(\beta, \gamma) \leftarrow (\frac{rt}{m + t'}, \frac{ms - \omega(r + s)m'}{\omega(m + t)m'} - \frac{\alpha}{\omega m'})$

$$r^* \leftarrow m^\alpha r^\beta g^\gamma \pmod{p} \quad \xrightarrow{m', r^*}$$

(4) \xleftarrow{d}

(5) $r' \leftarrow (r^* y)^d g^{-\frac{1}{m'}} \pmod{p}$

$r' \leftarrow (r^* y)^d g^{-\frac{1}{m'}} \pmod{p}$

if $dr' = 0 \pmod{q}$ then repeat from step (1).

(6) $(a, b) \leftarrow (\alpha d, \beta d)$

(7) $(s', t') \leftarrow (\frac{art - bms}{\text{wrt}} r' \pmod{q}, -m') \xrightarrow{s', t'} \text{accept if } \text{verify}(y, m', (r', s', t'))$

Fig. 2. Transforming a signature